From the twitter feed…
Denial of Service Attacks and
A Social Network Directory UPDATE

by
Lt Col Kristal Alfonso
Air Force Research Institute

UPDATED: Recently, Twitter, Facebook, Live Journal, and Blogger suffered Denial of Service (DoS) attacks that overloaded their systems to the point that Twitter's site went down for several hours and Facebook's site, although available, was extremely slow. This past week, Twitter users again endured another short outage of service, while Facebook suffered a repeat of a slower service.

While the news of the first DoS attack immediately circulated the "techie" blogs and traditional media sources, information about whom or what was behind the attacks continues to unfold. It initially appears that a blogger from Georgia was the focus of the first attack, which occurred on the 1-year anniversary of the start of the Georgian-Russian conflict over Ossetia.[i] Coverage of the second attack received far less attention and has taken a back seat to news reports on a lawsuit brought against Facebook over privacy concerns. While privacy is always a challenge in regards to on-line activity, the DoS attacks need to remain on the radar scope of anyone using social networking sites.

Ironically, the DoS attacks coincided with news that the Pentagon has begun a review of social network usage. While the concern over security continues to and should guide DoD policies, and that of the individual services, perhaps attention should also be paid to another aspect of these events. In conjunction with determining the best ways to defend against DoS attacks that exploit social networking sites and users, perhaps the DoD should also consider the benefits of using social networks for their potential offensive capabilities.

During the June 2009 civil unrest in Iran, for example, social networks were used to encourage protestors to learn how to perform social cyber unrest.[ii] The social cyber unrest targeted government websites in order to conduct DoS

attacks. Social networks provide an effective tool to recruit, educate, and organize the cyber activities of a "cyber army." There is an important lesson in this case that the DoD should examine: anyone can effectively serve in a "cyber army."

If the DoD chose to regard all uniformed and civilian employees as part of a greater, active DoD "cyber force," in lieu of viewing them merely as users, cyber experts could train and prepare the force to conduct cyber operations against potential adversaries in addition to defending the DoD network. Furthermore, a better trained and armed "cyber force" would expand our abilities to defend against cyber attacks. The current computer based training simply does not provide the robust education needed to become an effective "cyber force."

Even if DoD decides to ban all official access to social networks, training and education still needs to occur. Since many DoD personnel interact with the cyber domain from the personal systems, including their iPhones, Palm Pilots, and Blackberries, on a pretty consistent basis, the need to educate DoD personnel on how to navigate social networks remains paramount. Currently, there are some organizations developing guidelines to help users, but in the mean time, here is a short list of suggestions to help protect your computer as you navigate social networks.

Protect Your Profile: Denial of service attacks often use computers that have been unknowingly hijacked through the spread of malware. These systems are often linked and "botted" to launch attacks simultaneously unbeknownst to the computer's owner via the malware that users have unwittingly downloaded.

If you are entering into the social network for the first time or have been using various social network media, here are some security recommendations from experts from around the cyber galaxy to protect yourself, your friends, and your network. These tips are not final solutions or fool proof; but hopefully, they will help ensure that your adventure into social networking remains a positive experience. Use them to begin your education on cyber situational awareness and as a springboard for further research on the subject.

1. **Log off:** Make sure you log off from social network sites when you are done using them. This includes sites such as Facebook, Twitter, Youtube, MySpace, etc. but also includes sites such as Yahoo, MSN, and Google

where you can remain logged in indefinitely. Certain worms and viruses need you to be logged on in order to spread their malware. By logging off when not in use, you reduce your profile exposure to those who would seek to exploit it.[iii]

2. **Re-examine your password:** Most likely, it is not strong enough. Furthermore, if you use the same password for multiple social networks, you are making it easier for someone to gain access to your profiles.
3. **Watch third-party applications:** Popular "apps" often come in the form of games, polls, and user interface modifications. These apps can have malware hidden in them that users confuse for honest software.
    - A worm virus that Facebook users have had to deal with recently, Koobface, poses as a "flash download" required to view a link offered by a "friend." In reality, the "friend" had unwittingly downloaded the worm which then has converted their profile and computer into a "bot" to spread the virus further. As long as they were logged on, the bot can send out notices to friends within their network encouraging them to open the link and download the malware.
4. **Be careful when opening links** provided through social networks, even if they are provided from what appear to be trusted sources. Malware programmers often attempt to make their viruses look like legitimate software by presenting it in an official capacity. The Koobface virus, for instance, prompts the user to download an updated version of Flash Player (flash_player.exe) and the recent attempt to use a fraudulent CNN.com website to foist the "cease-fire Trojan attack" on unsuspecting users.
5. **Scan your system frequently:** We are often reminded about backing our systems up in order to avoid losing precious information (and there are even companies out there who will do it for you) but then choose to rely on security software to protect that precious information. This can lead to a false sense of security. Take your defenses to the next level and actively participate in defending your network. For example, during a recent scan of my own personal computers, two out of the three

systems had malware buried in them which my normal security programs did not identify and remove. It was only by actively scanning the systems using a different security program did we discover the malware. If you have questions about security software programs and how to scan your own system, your organization's computer experts are a good starting point for information.

- There is an assumption that the primary focus of malware miscreants remains on users of Windows; however, recent evidence has indicated that those using Mac and Linux are also at risk. To quote an expert in the field, "It is becoming quite pervasive."[iv]

6. **Pay attention to warning pop-ups:** If you frequently surf the internet, you may have become complacent when pop-ups warn you about entering into or downloading from questionable websites. Make sure you read and understand what you are agreeing to before proceeding.
7. **Maintain your firewall and keep your security protocols up to date:** Internet Explorer 8 and Firefox, for example, have developed more robust capabilities to help you combat attempts to gain access to your system. However, firewalls do not prevent nor catch everything, so remain vigilant and actively engage in your own security operations. This would include ensuring that your spyware/security programs are also current and up to date.
8. **Educate yourself:** There are various websites that can help you wade through the security dilemma of cyberspace. Wired.com and pcworld.com are good starting places to begin your education on the various security considerations and systems available to you.
9. **Do not be deterred:** Treat cyberspace like you would when driving down the highway. Become a defensive driver in cyberspace. Educate, protect, and enjoy. Choosing to not go on or use the valuable information that is out there merely accomplishes what an adversary seeks to do.

Social Network Directory

Below is a compilation (granted somewhat partial) of Air Force twitter feeds “The Wright Stuff” currently follows:

@au_wrightstuff

@AFRI09: Air Force Research Institute

@afsymposiums: Air Force Symposium Series

@afspace: Space Command

@afpaa: Air Force Public Affairs

@MobilityAirmen: AMC

@USAFBand

@NellisAFB

@MaxwellAFB

@45SpaceWingPA

@AF_ISRAgency

@noradnorthcom

@AFRC

@AFMC_Now

@US_Air_Force

@airforcelive

@USAFThunderbird

@HometownNews1

@airforcerotc

Here are some additional DoD-related twitter handles that "The Wright Stuff" follows:

@smallwars: Small Wars Journal

@dangerroom: Wired.com's defense related news feed

@southcomwatch

@EUCOM_QL

@thejointstaff: Adm. Mullen's twitter feed (he also has a Facebook page)

@RUSI_org: Royal United Services Institute (Great Britain)

@defenselink_mil

@pentagonchannel

@USArmyEurope

@usfora: US Force Afghanistan (there is also a Facebook page)

@govtwit: government twitter directory

Another excellent source for information on social networking and associated websites can be found at http://www.af.mil/shared/media/document/AFD-090406-036.pdf. Look for a future consolidated list from Air Force Public Affairs to provide users a one stop shop resource. In the mean time, they suggest interested individuals can also check out http://govtwit.com/.

The following are additional social network sites operated by or associated with the Air Force:

YouTube: http://www.youtube.com/AFBlueTube

Facebook: http://www.facebook.com/home.php?#/profile.php?id=1409442190&ref=name

AirForceLive blog: http://airforcelive.dodlive.mil/

Delicious: http://www.delicious.com/SAFPA

Digg: https://www.digg.com/safpa

FriendFeed: http://friendfeed.com/usairforce

Great Americans: http://www.greatamericans.com/afbluetube

If there are other links that you think "The Wright Stuff" and its staff should follow, please feel free to contact us with your recommendations or let this author know through her twitter feed @hellocatrine or through Facebook.

UPDATED: Here are some Air Force additional websites and Facebook groups related to social media:

@AFOSR: Air Force Office of Science and Research

@MSFRIC: Air University's Muir S. Fairchild Research Information Center

@AFCareers: AFPC

@USAFFutureLearn: USAF Future Learning Office

@1stCombatCamera: Changed from @AFCombatCamera; can also be found on Facebook and Youtube at 1stCombatCamera

Air University's Cyberspace and Information Operations Study Center: http://www.au.af.mil/info-ops/socialmedia.htm

AETC: http://www.facebook.com/pages/Randolph-Air-Force-Base-TX/Air-Education-and-Training-Command/105233234493?ref=ts

Air Force on Facebook: http://www.facebook/com/Usairforce

You can also become a fan of or join the following groups: “Air University’s The Wright Stuff”, “School of Advanced Air and Space Studies”, and “Air Force” on Facebook.

Lt Col Kristal Alfonso, a 2008 graduate of Air University’s School of Advanced Air and Space Studies, is a defense analyst at the Air Force Research Institute concentrating in new/emerging/social media. The views represented here are solely those of the author and do not necessarily reflect the views and policies of the US Air Force or the Department of Defense.

---

[i] http://www.networkworld.com/news/2009/080709-twitter-dos-attack-targeted-georgian.html
[ii] http://www.networkworld.com/news/2009/061809-twitter-plays-key-role-in.html?page=2
[iii] http://antivirus.about.com/od/securitytips/ht/koobface.htm
[iv] Mr. Larry R. McMaster, Precision Fires Program Manager, Research Triangle Institute International